

## **REMARKS**

The Office Action dated April 1, 2009, has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 1-4, 7-22, and 25-28 are currently pending in the application, of which claims 1, 11-13, and 18-19 are independent claims. Claims 13-17 have been amended to more particularly point out and distinctly claim the invention. No new matter has been added. Claims 1-4, 7-22, and 25-28 are respectfully submitted for consideration in view of the following remarks.

Claims 1-4, 7, 9, 11-14, 18-22, 25, and 27 were rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Application Publication No. 2003/0084300 of Koike ("Koike"). Applicants respectfully traverse this rejection.

Claim 1, upon which claims 2-4 and 7-10 depend, is directed to a method including receiving at a broker a usage policy for constraints related to data of a user in a communication system, wherein said usage policy defines at least one strictness level parameter value for at least one attribute in the usage policy. The method also includes receiving a request for data associated with the user from a service provider in the communication system to the broker, wherein the service provider possesses a privacy policy and wherein said request comprises at least one strictness level parameter value for at least one attribute in the privacy policy. The method further includes checking, in the broker, the request against a usage policy of the user by comparing strictness level

parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes in the privacy policy. The method additionally includes sending a response to the service provider indicating whether the data can be released, based on the comparison of the strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes the privacy policy.

Claim 11 is directed to a system including a service provider possessing a privacy policy. The system also includes a broker hosting a usage policy for constraints related to data of a user, wherein said usage policy defines at least one strictness level parameter value for at least one attribute in the usage policy, wherein the broker is configured to check a request from the service provider against the usage policy of the user by comparing strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes in the privacy policy, wherein said request comprises at least one strictness level parameter value for at least one attribute in the privacy policy, and the broker is configured to send a response to the service provider indicating whether data associated with the user can be released in response to the request based on the comparison of the strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes the privacy policy.

Claim 12 is directed to a system including introducing means for introducing to a broker a usage policy for constraints related to data of a user, wherein said usage policy defines at least one strictness level parameter value for at least one attribute in the usage policy. The system also includes receiving means for receiving a request for data associated with the user from a service provider to the broker, wherein the service provider possesses a privacy policy and wherein said request comprises at least one strictness level parameter value for at least one attribute in the privacy policy. The system further includes checking means for checking, in the broker, the request against a usage policy of the user by comparing strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes in the privacy policy. The system additionally includes sending means for sending a response to the service provider indicating whether the data can be released, based on the comparison of the strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes the privacy policy.

Claim 13, upon which claims 14-17 depend, is directed to an apparatus including at least one memory including computer code and at least one processor. The at least one memory and the computer program code are configured to, with the at least one processor, cause the apparatus at least to receive a request for data associated with a user from a service provider, wherein the service provider possesses a privacy policy and wherein said request comprises at least one strictness level parameter value for at least

one attribute in the privacy policy. The at least one memory and the computer program code are also configured to, with the at least one processor, cause the apparatus at least to check the request against a usage policy of the user by comparing strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes in the privacy policy, wherein said usage policy defines at least one strictness level parameter value for at least one attribute in the usage policy. The at least one memory and the computer program code are further configured to, with the at least one processor, cause the apparatus at least to send a response to the service provider indicating whether the data can be released, based on the comparison of the strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes the privacy policy.

Claim 18 is directed to an apparatus including receiving means for receiving a request for data associated with a user from a service provider, wherein the service provider possesses a privacy policy and wherein said request comprises at least one strictness level parameter value for at least one attribute in the privacy policy. The apparatus also includes checking means for checking the request against a usage policy of the user by comparing strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes in the privacy policy, wherein said usage policy defines at least one strictness level parameter value for at least one attribute in the usage policy. The

apparatus further includes sending means for sending a response to the service provider indicating whether the data can be released, based on the comparison of the strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes the privacy policy.

Claim 19, upon which claims 20-22 and 25-28 depend, is directed to a computer-readable medium comprising computer-executable components. The components are configured to receive a usage policy for constraints related to data of a user in a communication system, wherein said usage policy defines at least one strictness level parameter value for at least one attribute in the usage policy. The components are also configured to receive a request for data associated with the user from a service provider in the communication system, wherein the service provider possesses a privacy policy and wherein said request comprises at least one strictness level parameter value for at least one attribute in the privacy policy. The components are further configured to check the request against a usage policy of the user by comparing strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes in the privacy policy. The components are additionally configured to send a response to the service provider indicating whether the data can be released, based on the comparison of the strictness level parameter values associated with attributes in the usage policy to corresponding

strictness level parameter values associated with corresponding attributes the privacy policy.

Applicants respectfully submit that Koike fails to disclose or suggest all of the elements of any of the presently pending claims.

Koike generally relates to a system for administrating data including privacy of a user in communication made between a server and the user's terminal device. The system of Koike includes a server, a terminal device owned by the user, and a privacy data administrator connected between the server and the terminal device. The privacy data administrator, in Koike, compares a privacy policy made by the server and privacy preference determined by the user to each other, and determines whether the privacy data administrator is allowed to provide data, including privacy of the user, to the server.

Claim 1 recites, in part, "sending a response to the service provider indicating whether the data can be released, based on the comparison of the strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes the privacy policy." Applicants respectfully submit that Koike does not disclose or suggest at least these features of claim 1.

The Office Action's discussion of Koike does not address the issue of using strictness level parameter values for attributes in privacy and usage policies, as such. It is respectfully submitted that Koike does not contain such discussion.

At section 4, the Office Action responded to this distinction. The Office Action stated that “Koike expressly discloses that when it is determined that the data can be sent to the service provider, a response is submitted to the service provider.” In order for this to be responsive to the distinction that Koike does not address the issue of using strictness level parameter values for attributes in privacy and usage policies, as such, the Office Action must have been taking the implicit position that every determination that data can be sent to the service provider includes using strictness level parameter values for attributes in privacy and usage policies. Such, however, is not the case. This can be seen from the very example paragraphs cited by the Office Action.

In paragraph [0135] Koike bases its transmission decision not on strictness level parameter values for attributes in privacy and usage policies but rather on “whether the privacy policy 30b is acceptable to the user.” Paragraph [0097] discusses transmitting (apparently unconditionally) data about a user’s privacy to a privacy data administrator. Finally, paragraph [0084] of Koike mentions a transmission decision not based on strictness level parameter values for attributes in privacy and usage policies but “based on a privacy policy presented from the server ... and a privacy preference having been established in advance by the user.” These determinations, where there are determinations, are possible without a “comparison of the strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes the privacy policy” as recited, for example, in claim 1.

More significantly, however, none of these paragraphs mention any “sending a response to the service provider indicating whether the data can be released,” as recited in claim 1. Instead, they mention the provision of privacy preferences and decisions based on those preferences, but no responses that indicate whether data can be released. Thus, it is respectfully submitted that the rejection cannot be maintained, and withdrawal of the rejection is respectfully requested.

Even assuming that Koike disclosed providing a response to a service provider indicating whether data can be released (not admitted), there is no discussion in Koike of a “comparison of the strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes the privacy policy.” Thus, the features of claim 1 are clearly distinguishable over Koike.

At item 5, the Office Action responded to the distinction identified above. The Office Action argued that Koike mentions that data is administered in accordance with P3P standards. Furthermore, the Office Action argued that Koike defines various strictness levels. Finally, the Office Action argued that Koike discloses “a comparator which compares the privacy policy to the privacy preference and judges whether the privacy policy is consistent with the privacy preference,” citing paragraph [0090]. The Office Action then concluded that the claim recitations are met. Applicants respectfully submit that the Office Action’s rationale is flawed.



Koike does mention that a comparison is made between privacy preferences and a privacy policy. Koike's reason for doing this is to determine whether a privacy policy is acceptable to a user of the terminal device as explained at paragraph [0089]. Koike does not state that the way in which the comparison for consistency is made is by comparing "strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes the privacy policy" and there is nothing provided in the Office Action that indicates that P3P requires that the comparison be done this way, whether or not elements in P3P can be arranged according to strictness.

Furthermore, as noted in the present application at paragraphs [0009] and [0010], the features of using strictness level parameter values for attributes in privacy and usage policies can advantageously allow for an easy way to check the matching or non-matching between different policies. Thus, the features of claim 1 are not only novel, but non-obvious with respect to Koike.

Additionally, it should be noted that the response(s) relied-upon in Koike is/are not a "response to the service provider indicating whether the data can be released," as recited in claim 1. Instead the most relevant response in Koike is a response that actually transmits data from the terminal device 120 of the user, to the server 110 (paragraphs [0084] and [0135]). The other response is the user transmitting requested data about the user's privacy to the privacy data administrator (paragraph [0097]). Neither of those responses is a "response to the service provider indicating whether the data can be

released,” as recited in claim 1. Thus, even if the citation of paragraphs [0084], [0097], and [0135] were able to address the deficiencies identified above, the responses used to address those deficiencies would simply raise new and further deficiencies. Accordingly, the rejection cannot be maintained on the grounds provided and withdrawal of the rejection is respectfully requested.

Although independent claims 11-13 and 18-19 each have their own respective scope, each recites at least some features similar to those discussed above with respect to claim 1. It is, therefore, respectfully requested that, for similar reasons, the respective rejections of each of claims 1, 11-13, and 18-19 be withdrawn.

Claims 2-4, 7, 9, 14, 20-22, 25, and 27 depend respectively from, and further limit claims 1, 13, and 19. Each of claims 2-4, 7, 9, 14, 20-22, 25, and 27, therefore, recites subject matter that is neither disclosed nor suggested in Koike. It is, therefore, respectfully requested that the rejection of claims 2-4, 7, 9, 14, 20-22, 25, and 27 be withdrawn.

Claims 1-4, 7, 11-14, 18-22, and 25 were rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Application Publication No. 2003/0088520 of Bohrer et al. (“Bohrer”). Applicants respectfully traverse this rejection.

The independent claims are discussed above. Bohrer generally relates to a system, method, and business method for enforcing privacy preferences on personal-data exchanges across a network. In Bohrer, there are one or more data-subject rule sets that have one or more subject constraints on one or more private, subject data releases. A

receiving process, in Bohrer, requires a request message from a data-requester over a network interface. The request message includes at least one request for one or more of the private, subject data releases pertaining to a subject, and a requester privacy statement for each of the respective private data. In Bohrer's system, a release process compares the requester privacy statement to the subject constraints and releases the private, subject data release in a response message to the requestor only when the subject constraints are satisfied.

Claim 1 recites, in part, "sending a response to the service provider indicating whether the data can be released, based on the comparison of the strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes the privacy policy." Applicants respectfully submit that Bohrer does not disclose or suggest at least these features of claim 1.

The Office Action's discussion of Bohrer does not address the issue of using strictness level parameter values for attributes in privacy and usage policies, as such. It is respectfully submitted that Bohrer does not contain such discussion.

Even assuming that Bohrer disclosed providing a response to a service provider indicating whether data can be released (not admitted), there is no discussion in Bohrer of a "comparison of the strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with

corresponding attributes the privacy policy.” Thus, the features of claim 1 are clearly distinguishable over Bohrer.

Furthermore, as noted in the present application at paragraphs [0009] and [0010], the features of using strictness level parameter values for attributes in privacy and usage policies can advantageously allow for an easy way to check the matching or non-matching between different policies. Thus, the features of claim 1 are not only novel, but non-obvious with respect to Bohrer.

Although independent claims 11-13 and 18-19 each have their own respective scope, each recites at least some features similar to those discussed above with respect to claim 1. It is, therefore, respectfully requested that, for similar reasons, the respective rejections of each of claims 1, 11-13, and 18-19 be withdrawn.

Claims 2-4, 7, 14, 20-22, and 25 depend respectively from, and further limit claims 1, 13, and 19. Each of claims 2-4, 7, 14, 20-22, and 25, therefore, recites subject matter that is neither disclosed nor suggested in Bohrer. It is, therefore, respectfully requested that the rejection of claims 2-4, 7, 14, 20-22, and 25 be withdrawn.

At sections 7-8, responding to the above distinctions, the Office Action appeared to argue similarly as with respect to the distinctions raised regarding Koike. Thus, the discussion above may also apply to the Office Action’s comments in these sections.

In particular, the Office Action cited paragraphs [0081] and [0088] as teaching “sending a data response back to the service provider containing the results of the data request.” Such teaching, however, is not equivalent to what is claimed. What is claimed

is not simply sending a response to a data request. The cited paragraphs refer to a process in which privacy declaration is compared to privacy preferences in a profile and data is returned when a match exists. However, such a determination does not necessarily involve “comparison of the strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes the privacy policy.” Thus, it is respectfully submitted that the rejection is improper, and withdrawal of the rejection is respectfully requested.

Additionally, it should be noted that the response(s) relied-upon in Bohrer is not a “response to the service provider indicating whether the data can be released,” as recited in claim 1. Instead the most relevant response in Bohrer is a response that actually provides the requested data, if permitted (paragraph [0081]). The other response is provides the data available to the server as well as any third party information required for the data requester (paragraph [0088]). Neither of those responses is a “response to the service provider indicating whether the data can be released,” as recited in claim 1. Thus, even if the citation of paragraphs [0081] and [0088] were able to address the deficiencies identified above, the responses used to address those deficiencies would simply raise new and further deficiencies. Accordingly, the rejection cannot be maintained on the grounds provided and withdrawal of the rejection is respectfully requested.

Claims 8, 15, and 26 were rejected under 35 U.S.C. 103(a) as being unpatentable over Bohrer. Applicants respectfully traverse this rejection.

Claims 8, 15, and 26 depend respectively from, and further limit claims 1, 13, and 19. At least some of the deficiencies of Bohrer with respect to claims 1, 13, and 19 are described above. The additional allegedly “notoriously well known” features asserted in the rejection are not related to the deficiencies identified above. Accordingly, for at least the same reasons set forth above, the rejections of claims 8, 15, and 16 should be withdrawn.

The Office Action alleged that “It is notoriously well known in the art to include as much detail of a transaction to maintain audit information for future analysis. Official notice of this teaching is taken.” Applicants respectfully traverse this Official Notice. It is notorious that memory in computer systems is limited. Therefore, common sense suggests not storing information that is not thought to be needed. There is nothing in Bohrer that suggests that the information in question would be needed, in fact Bohrer doesn’t even mention “a strictness level parameter value of an attribute of the usage policy to the service provider” nor does Bohrer envision the occasion “when the corresponding strictness level parameter value of the corresponding attribute of the privacy policy of the service provider is greater than the indicated strictness level parameter value of the attribute in the usage policy,” as recited in claim 8 or the corresponding features of claims 15 and 26, which each have their own respective scope. Thus, contrary to the Office Action’s assertion, the features of claims 8, 15, and 26 are not obvious in view of Bohrer.

Claims 9, 16, and 27 were rejected under 35 U.S.C. 103(a) as being unpatentable over Bohrer in view of Koike. Applicants respectfully traverse this rejection.

Claims 9, 16, and 27 depend respectively from, and further limit, claims 1, 13, and 19. At least some of the deficiencies of Bohrer and Koike with respect to claims 1, 13, and 19. Because Bohrer and Koike share at least some of the deficiencies with respect to claims 1, 13, and 19 the combination of Bohrer and Koike likewise fails to disclose or suggest all of the elements of claims 1, 13, and 19 or of claims 9, 16, and 27, which depend therefrom. It is, therefore, respectfully requested that the rejection of claims 9, 16, and 27 be withdrawn.

Claims 10, 17, and 28 were rejected under 35 U.S.C. 103(a) as being unpatentable over Koike in view of U.S. Patent Application Publication No. 2005/0086061 of Holtmanns et al. (“Holtmanns”). The Office Action acknowledged that Koike fails to disclose at least some of the further limitations of the claims, and cited Holtmanns to remedy Koike’s deficiencies. Applicants respectfully traverse this rejection.

Claims 10, 17, and 28 depend respectively from, and further limit, claims 1, 13, and 19. At least some of the deficiencies of Koike with respect to claims 1, 13, and 19 are discussed above. Holtmanns fails to remedy the above-identified deficiencies of Koike, and consequently the combination of Koike and Holtmanns fails to disclose or suggest all of the elements of any of the presently pending claims.

Holtmanns generally relates to a method and apparatus for personal information access control. Nevertheless, Holtmanns does not disclose or suggest, “sending a

response to the service provider indicating whether the data can be released, based on the comparison of the strictness level parameter values associated with attributes in the usage policy to corresponding strictness level parameter values associated with corresponding attributes the privacy policy,” as recited in claim 1. Thus, Holtmanns does not remedy the above-identified deficiencies of Koike, and the combination of Koike and Holtmanns fails to disclose or suggest all of the elements of claims 1, 13, and 19. It is, therefore, respectfully requested that the rejection of claims 10, 17, and 28 be withdrawn.

Claims 10, 17, and 28 were also rejected under 35 U.S.C. 103(a) as being unpatentable over Bohrer in view of Holtmanns. The Office Action acknowledged that Bohrer fails to disclose at least some of the further limitations of the claims, and cited Holtmanns to remedy Bohrer’s deficiencies. Applicants respectfully traverse this rejection.

Claims 10, 17, and 28 depend respectively from, and further limit, claims 1, 13, and 19. At least some of the deficiencies of Bohrer with respect to claims 1, 13, and 19 are discussed above. Holtmanns fails to remedy the above-identified deficiencies of Bohrer, and consequently the combination of Bohrer and Holtmanns fails to disclose or suggest all of the elements of any of the presently pending claims.

Holtmanns generally relates to a method and apparatus for personal information access control. Nevertheless, Holtmanns does not disclose or suggest, “sending a response to the service provider indicating whether the data can be released, based on the comparison of the strictness level parameter values associated with attributes in the usage



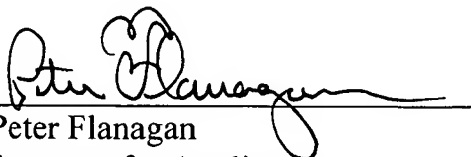
policy to corresponding strictness level parameter values associated with corresponding attributes the privacy policy,” as recited in claim 1. Thus, Holtmanns does not remedy the above-identified deficiencies of Bohrer, and the combination of Bohrer and Holtmanns fails to disclose or suggest all of the elements of claims 1, 13, and 19. It is, therefore, respectfully requested that the rejection of claims 10, 17, and 28 be withdrawn.

For the reasons set forth above, it is respectfully submitted that each of claims 1-4, 7-22, and 25-28 recites subject matter that is neither disclosed nor suggested in the cited art. It is, therefore, respectfully requested that all of claims 1-4, 7-22, and 25-28 be allowed, and that this application be passed to issuance.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the Applicants’ undersigned representative at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, Applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Peter Flanagan", is written over a horizontal line.

Peter Flanagan  
Attorney for Applicants  
Registration No. 58,178

**Customer No. 32294**  
SQUIRE, SANDERS & DEMPSEY L.L.P.  
14<sup>TH</sup> Floor  
8000 Towers Crescent Drive  
Vienna, Virginia 22182-6212  
Telephone: 703-720-7800  
Fax: 703-720-7802

PCF:dlh

Enclosures: Petition for Extension of Time  
Check No. 21127